Warnung vor aktiver Spam-Kampagne: Angebliche Corona-Arbeitsschutzregeln enthalten Schadsoftware

Eine Mail, die angeblich vom Bundesgesundheitsministerium stammt, enthält einen Downloader für eine Schadsoftware. Der Dateianhang mit dem Namen "Bund-Arbeitsschutzregel-Corona-September.zip" enthält vorgeblich ein Dokument mit aktualisierten und ab sofort verbindlichen Regeln für den Infektionsschutz am Arbeitsplatz. Der Text der Mail lässt den Schluss zu, dass in erster Linie Unternehmen zur Zielgruppe gehören. Aus diesem Grund ist momentan für Unternehmen besondere Vorsicht geboten, wenn vermeintliche Mails von Behörden im Postfach landen. Uns sind Berichte über derzeit aktive Infektionen bekannt.

"Die Corona-Pandemie sorgt noch immer für viel Unsicherheit - und die Mischung aus viel Homeoffice und Hygieneregeln am Arbeitsplatz stellt Arbeitgeber tatsächlich vor große Herausforderungen", sagt Tim Berghoff, Security Evangelist bei G DATA CyberDefense. "Gerade deshalb sollten die Verantwortlichen aber sehr genau hinschauen und nur offiziellen Quellen vertrauen. Denn eine Infektion mit Schadsoftware können Unternehmen im Moment noch weniger gebrauchen, als ohnehin schon."

Der Text der Mail weist auf ein Treffen zwischen den Gesundheitsministern der EU hin, bei dem die aktualisierten Vorschriften überarbeitet worden seien. Dass es solch ein Treffen gegeben hat, mag vielleicht sogar stimmen - allerdings werden solche Informationen in der Regel nicht per Mail von den Ministerien versendet, sondern auf einem eigenen Portal veröffentlicht. Es findet kein proaktiver Versand per Mail statt.

Des Weiteren nimmt der Mailtext Bezug auf ein Treffen, welches "heute" stattgefunden habe. Es befinden sich auch einige Zeichenfehler in der Mail, vor allem den Buchstaben U, W, C und D sowie bei Umlauten. Die Mail enthält auch eine falsche Absendeadresse, die auf "bundesministerium-gesundheit.com" verweist - diese Domain gehört jedoch nicht zum Gesundheitsministerium. Die im Mailtext erwähnte Adresse "poststelle@bmg.bund.de" ist jedoch tatsächlich korrekt.

Um sich vor einer Schadsoftwareinfektion aus einer solchen Mail zu schützen, sollten Unternehmen und Privatpersonen alle Informationen rund um die COVID-19-Pandemie und entsprechende Schutzmaßnahmen ausschließlich aus offiziellen Quellen beziehen. Alle aktuellen Informationen rund um Corona und COVID-19 sind auf der Internetseite des Bundesministeriums für Gesundheit (BmG) gesammelt.

Eine weitere Mail mit identischer Schadfunktion ist übrigens derzeit in Form eines gefälschten Bewerbungsschreibens unterwegs. Einer der verwendeten Namen für die vermeintliche Bewerbung lautet "Claudia Alick".

Das Kriminelle die Pandemie als Hebel für ihre Aktivitäten nutzen, ist nicht neu: bereits zu Beginn der Pandemie haben Betrüger dafür gesorgt, dass die Auszahlung von Finanzhilfen für gefährdete Unternehmen kurzzeitig ausgesetzt wurde.

Schadfunktionen

Nach bisherigen Erkenntnissen enthält der Mailanhang einen JScript-Loader namens "Buer" - dieser wiederum lädt aus dem Internet eine weitere Schadsoftware nach. Bei dieser handelt es sich um NuclearBot - ein Bankingtrojaner, der es unter anderem auf die Passwörter von Bankkonten abgesehen hat. Diese Schadsoftware ist für uns keine Unbekannte - wir hatten vor einiger Zeit bereits mit ihr Berührung und haben darüber ebenfalls einen Blog-Artikel geschrieben: